AMENDMENTS TO THE CLAIMS

Please find below a complete listing of the claims in the application, including their status as effected by the present amendment:

1. (*currently amended*) A system for analyzing network traffic comprising:
   - a plurality of subscriber units and a default router [[~~default router~~]] interconnected by a first network, said first network operable to direct routed traffic to an appropriate subscriber unit and further operable to direct unrouted traffic to said default router [[~~default route generator~~]]; and
   - an analyzer connected to said default router [[~~default router~~]] for determining a misconfiguration of a network routing table in a second network adjacent to said first network based on patterns of activity within said unrouted traffic.

2. (*cancelled*)

3. (*cancelled*)

4. (*currently amended*) The system according to claim [[~~3~~]] 1, wherein said misconfiguration [[~~is a~~]] results [[~~of~~]] in said second network routing traffic to a third network adjacent said first network via said first network.

5. (*currently amended*) The system according to claim [[~~3~~]] 1, wherein said misconfiguration is a breach of a service contract between an operator of said first network and an operator of said second network.

6. (*original*) The system according to claim 5 further comprising a means for assessing a penalty against an operator of said second network, said penalty corresponding to said breach of contract.

7. (*cancelled*)

8. (*cancelled*)

9. (*cancelled*)

10. (*cancelled*)

11. (*original*) The system according to claim 1 further comprising a honey pot connected to said analyzer for responding to said unrouted traffic.

12. (*original*) The system according to claim 11 wherein said honey pot is operable to permit itself to be infected with a malicious code associated with said unrouted traffic.

13. (*currently amended*) The system according to claim 12 wherein said honey pot includes a malicious code scanner for identifying said malicious code once said honey pot [[~~computer~~]] is infected.

14. (*cancelled*)

15. (*cancelled*)

16. (*original*) The system according to claim 15 further comprising a means for charging a fee to a subscriber associated with said one of said subscriber units.

17. (*original*) The system according to claim 1 further comprising a means for providing said analyzer with updated definitions of known patterns of malicious traffic.

18. (*currently amended*) A traffic analyzer comprising:

- an interface for connecting to a <u>first</u> network, said network operable to interconnect a plurality of subscriber units, said <u>first</u> network further operable to direct routed traffic to an appropriate subscriber unit and further operable to direct unrouted traffic to said interface; and,
- a processing means connected to said interface, said processing means operable to determine <u>a misconfiguration of a network routing table in a second network adjacent to said first network based on</u> patterns of activity within said unrouted traffic.

19. (*cancelled*)

20. (*cancelled*)

21. (*currently amended*) The analyzer according to claim [[20]] 18, wherein said misconfiguration [[~~is a~~]] result~~s~~ [[~~of~~]] in said second network routing traffic to a third network adjacent said first network via said first network.

22. (*currently amended*) The analyzer according to claim [[20]] 18, wherein said misconfiguration is a breach of a service contract between an operator of said first network and an operator of said second network.

23. (*cancelled*)

24. (*cancelled*)

25. (*cancelled*)

26. (*cancelled*)

27. (*original*) The analyzer according to claim 18 further comprising a honey pot connected to interface analyzer for responding to said unrouted traffic.

28. (*original*) The analyzer according to claim 27 wherein said honey pot is operable to permit itself to be infected with a malicious code associated with said unrouted traffic.

29. (*currently amended*) The analyzer according to claim 28, wherein said honey pot includes a malicious code scanner for identifying said malicious code once said honey pot [[~~computer~~]] is infected.

30. (*cancelled*)

31. (*cancelled*)

32. (*original*) The analyzer according to claim 18 further comprising a means for providing said analyzer with updated definitions of known patterns of malicious traffic.

33. (*currently amended*) The analyzer according to claim 18 wherein said interface is a default router operable to instruct a routing table associated with said first network to deliver unrouted traffic to said default router [[~~generator~~]].

34. (*cancelled*)

35. (*cancelled*)

36. (*cancelled*)

37. (*currently amended*) A method of analyzing traffic in a first network comprising the steps of:

- receiving traffic from at least one of a plurality of subscriber units interconnected by said first network;
- delivering said traffic to a destination subscriber unit if said traffic is routed;
- analyzing said traffic to determine a misconfiguration of a network routing table in a second network adjacent to said first network based on [[~~for~~]] patterns of activity in said traffic if said traffic is unrouted.

38. (*cancelled*)

39. (*cancelled*)

40. (*currently amended*) The method according to claim [[~~39~~]] 37, wherein said misconfiguration [[~~is a~~]] results [[~~of~~]] in said second network routing traffic to a third network adjacent said first network via said first network.

41. (*currently amended*) The method according to claim [[~~39~~]] 37, wherein said

misconfiguration is a breach of a service contract between an operator of said first network and an operator of said second network.

42. (*original*) The method according to claim 41 further comprising the step of assessing a penalty against an operator of said second network, said penalty corresponding to said breach of contract.

43. (*cancelled*)

44. (*cancelled*)

45. (*cancelled*)

46. (*cancelled*)

47. (*original*) The method according to claim 37 further comprising the step of responding to said unrouted traffic.

48. (*currently amended*) The method according to claim 47, further comprising the step of permitting an infection in a honey pot computer of a malicious code [[~~in~~]] associated with said unrouted traffic.

49. (*currently amended*) The method according to claim 48 further comprising the step of, after said permitting step, scanning said honeypot computer to identify said malicious code [[~~once~~]].

50. (*cancelled*)

51. (*cancelled*)

52. (*original*) The method according to claim 51 further comprising the step of charging a fee to a subscriber associated with said one of said subscriber units.

53. (*original*) The method according to claim 37 further comprising the step of providing updated definitions of known patterns of malicious traffic.

54. (*cancelled*)

55. (*cancelled*)

56. (*cancelled*)

57. (*currently amended*) A system for analyzing network traffic comprising:

- a first network;
- a plurality of subscriber units connected to said first network;
- a default router connected to said first network;
- a network router for directing traffic that is: addressed to one of said subscriber units to a corresponding said subscriber unit; and unaddressed to any said subscriber unit to said default router [[~~generator~~]];
- an analyzer connected to said default router for determining a misconfiguration of a network routing table in a second network adjacent to said first network based on patterns of activity within traffic directed to said default router [[~~generator~~]].

58. (*cancelled*)